

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor(s): **Randolph Michael Forlenza and Miguel Sang**

For: **EXTENSION OF BROWSER WEB PAGE CONTENT LABELS AND PASSWORD CHECKING TO COMMUNICATIONS PROTOCOLS**

Enclosed are:

- ☒ Patent Specification and Declaration
- ☒ 3 sheets of drawing(s).
- ☒ An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).
- ☐ A certified copy of a ☐ application.
- ☐ Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				\$690.00
Total Claims	21 - 20	1	x 18 =	\$ 18.00
Indep. Claims	6 - 3	3	x 78 =	\$234.00
MULTIPLE DEPENDENT CLAIM PRESENTED			x 260 =	\$
TOTAL				\$942.00

- ☒ Please charge IBM Corporation Deposit Account No. 09-0447 in the amount of \$942.00. A duplicate copy of this sheet is enclosed.
- ☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 09-0447. A duplicate copy of this sheet is enclosed.
- ☒ Any additional filing fees required under 37 CFR §1.16.
- ☒ Any patent application processing fees under 37 CFR §1.17.

**CERTIFICATE OF MAILING BY "EXPRESS MAIL"
UNDER 37 CFR § 1.10**

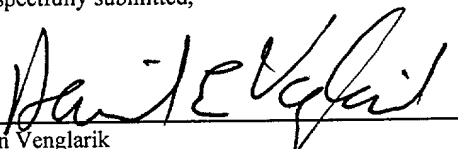
"Express Mail" mailing label number: **EL497382204US**

Date of Mailing: April 14, 2000

I hereby certify that the documents indicated above are being deposited with the United States Postal Service under 37 CFR 1.10 on the date indicated above and are addressed to Box Patent Applications, Assistant Commissioner for Patents, Washington, D.C. 20231 and mailed on the above Date of Mailing with the above "Express Mail" mailing label number.


Beth Costner

Respectfully submitted,

By 
Dan Venglarik
Registration No. 39,409 for
FELSMAN, BRADLEY, VADEN,
GUNTER & DILLON, LLP
201 Main Street, Suite 1600
Fort Worth, Texas 76102
Telephone (817) 332-8143

EXTENSION OF BROWSER WEB PAGE CONTENT LABELS AND
PASSWORD CHECKING TO COMMUNICATIONS PROTOCOLS

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates generally to data access control in data processing system networks and in particular to content-specific access control. Still more particularly, the present invention relates to extending existing content-specific access control mechanisms for Web pages to other communications protocols.

2. Description of the Related Art:

Conventional data access control is based on restricting access to specific servers, storage media (e.g., hard disk drives), directories, or files regardless of their content. That is, access to content is controlled by restricting access to the location of the content, such as by preventing a user from accessing (retrieving and viewing or executing) a file (or datastream) containing the content, rather than being based on the content itself. This type of access control generally involves setting file attributes within the file system or an access control list. However, such access control techniques are poorly suited for contemporary large scale publication of content on the Internet, where filenames (or streaming sources) are often generated electronically along with the content, and where content is frequently updated, so that tracking filenames

for content to be restricted is extremely complicated. It is also impossible for an individual unaware of the content of particular files to determine whether access to such files should be restricted.

5

There currently exists, for HyperText Transmission Protocol (HTTP) based systems, the ability for browsers to regulate, control and restrict the browsing of Web page content according to classifications contained in the content labels embedded in web pages. The content labels within a HyperText Markup Language (HTML) document, for example, are contained within a META tag for the document:

10

```
<META http-equiv="PICS-Label" content='(PICS-1.1
  <service url> [option...]
    labels [option...] ratings (<category> <value> ...)
      [option...] ratings (<category> <value> ...)
      ...
  <service url> [option...]
    labels [option...] ratings (<category> <value> ...)
      [option...] ratings (<category> <value> ...)
      ...
  ...)'>
```

15

20

The "PICS-1.1" reference is to a version of the content-labeling/rating protocol established by the Platform for Internet Content Selection, a working group affiliated with the World Wide Web Consortium (W3C). The protocol is described in greater detail at www.w3.org/PICS. Under this system, content labels are employed for either self-labeling by the content publisher or labeling by a rating service such as the Internet Content Rating Association (www.irca.org).

25

30

Content labels for HTML documents may be transmitted within the HTML document, with the HTML document in an HTTP (or other RFC-822-style protocol) header, or separately from the HTML document from a "label bureau," which is typically just an off-the-shelf HTTP server running a special Common Gateway Interface (CGI) script. The labels from a label bureau may refer to any document that has an associated Uniform Resource Locator (URL), including those available through protocols other than HTTP, such as File Transfer Protocol (FTP), Gopher, or NetNews (see RFC-1738).

HTTP content labels are most frequently employed in filtering systems, such as those integrated with browsers to prevent children from inadvertently accessing sexually explicit or graphically violent material. Access to certain types of content identified by content label may be restricted. Privileged users of a system assign passwords to certain content label categories and non-privileged users must supply the correct password to view a web page containing content encompassed by a restricted category.

Content-specific filtering is generally only enabled within the HTTP engine of a browser. Where only the browser on a system employs content-based filtering, it is possible for users to bypass the intent of the content restrictions when accessing non-HTTP data which does not contain content labels, or by utilizing non-HTTP protocols which do not support content restriction. For example, a user may retrieve binary image data containing sexually explicit content utilizing the FTP engine of a browser which does not provide content-based access control for non-HTTP protocols, or receive similar content as an attachments to an

electronic mail message. Alternatively, a non-privileged user may simply utilize the Network News reader program which is normally distributed with browsers. Even if the newsreaders supports content label-based access control, the privileged user (e.g., a parent) may not be sufficiently familiar with the Internet to understand that news groups also may contain sexually explicit or other undesirable material. These simple work-arounds can render existing browser content control methodologies ineffective.

It would be desirable, therefore, to allow privileged users, via password assignment, to further regulate, control, and restrict non-privileges user's ability to access, import, and export data external to the system or data within the system.

SUMMARY OF THE INVENTION

5 It is therefore one object of the present invention to provide improved data access control in data processing system networks.

10 It is another object of the present invention to provide improved content-specific data access control in data processing system networks.

15 It is yet another object of the present invention to extend existing content-specific data access control mechanisms for Web pages to other communications protocols.

20 The foregoing objects are achieved as is now described. Content label categories and associated user restrictions for desired access control may be entered by a privileged user in any communications programs (such as a browser) within a system, and are automatically distributed to all other communications programs (such as a different browser or a newsreader) within the system regardless of whether the same communications protocol is utilized. Communications programs being installed check for access control settings within other communications programs, and employ such
25 settings in configuring internal access controls. Content-based access control is thus implemented uniformly across the system without work arounds being available to the nonprivileged users. Content labels for requested content, which may be embedded within the requested content,
30 contained within a communications header for transactions bearing the requested content, or looked up in internal or external databases utilizing an identifier for the requested

AUS000072US1

content, are checked against content label categories restricted for a current user. If restricted content is detected, the user is prompted for a password before the requested content is displayed.

5

The above as well as additional objectives, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a data processing system network in which a preferred embodiment of the present invention may be implemented;

Figure 2 is a high level flow chart for a process of setting access control based on content labels in accordance with a preferred embodiment of the present invention; and

Figure 3 depicts a high level flowchart for a process of performing access control in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures, and in particular with reference to **Figure 1**, a data processing system network in which a preferred embodiment of the present invention may be implemented is depicted. Data processing system network 102 includes one or more servers 104-106 which are accessible as part of the Internet 108 or other network. Data processing system network 102 also includes one or more clients 110-112 which may access or receive content from servers 104-106. The content may be transmitted using any of a variety of protocols including HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), an electronic mail protocol such as IMAP or POP, or a local file system.

In accordance with the present invention, a client within data processing system network 102 such as client 112 includes functionality supporting different communications protocols for transmitting content, including a browser 114 (for HTTP communications), a news reader 116 (for Network News Transfer Protocol or NNTP communications), a mail program 118 (for IMAP or POP communications), and a file manager 120 (for local file storage and retrieval).

Although depicted in the exemplary embodiment as discrete function units, the functionality may be fully or partially integrated. For example, Netscape Navigator, available from AOL, Inc., includes browser, news reader, and mail functionality. Similarly, Internet Explorer, available from Microsoft Corporation, is tightly integrated with Windows Explorer, the file manager for the Windows 95, Windows 98,

and Windows 2000 operating systems, and also include support for mail functionality, although news reading is provided in a different program, Outlook Express. Additionally, other communications protocols such as gopher or WAIS may be supported within client 112.

Also included within client 112 in the exemplary embodiment is an access control module 122, a browser-based facility of the type similar to those associated with existing browser programs which permits a privileged user to regulate the accessibility of content label categories according to passwords assigned by the privileged user. In the present invention, however, the access control module 122 provides a single interface for establishing regulation of all communications protocols supported within client 112, not merely the browser or HTTP client. All communications protocols supported within client 112 (e.g., HTTP, FTP, NNTP, instant messaging protocol(s), MP3 or other media and/or streaming data player(s), and the operating system file system in the exemplary embodiment) provide access control based on content labels. Access control module 122 provides a single interface to all communications protocols supported within the system, allowing a privileged user to set content label-based access restrictions for all communications protocols supported within the system. The access control module 122 need not be browser-based as implemented within the exemplary embodiment. Instead, the access control mechanism and the associated user interface for setting access restrictions could be an integral part of the operating system, or part of a separate application.

AUS000072US1

To facilitate content-based access control, client 112 also includes user identifiers and passwords 124, as well as a "label bureau" 126a. Label bureau 126a provides content labels for locally stored content identified by filename, and may be part of the operating system file system, a simple table maintained separately from the file system, or some other implementation. Similar label bureau(s) 126b are located on content servers accessible to client 112, and provide content labels for content accessed by client 112 through the Internet 108 and identified by a uniform resource locator (URL).

Content labels for content accessed by client 112 may be determined in any of a variety of different manners. Content labels are preferably stored within or in association with content as metadata. For HTML content, existing content labeling may be employed. For other types of content, such as binary image data, content labeling may be implemented within comment or header portions of the content files. Alternatively, content labels may be maintained outside the files containing the content, either as an attribute of the file, metadata for the file, or simply within a separate file for content labels or as an attribute of the communications program. The content labels may then be transmitted within a header for a communications transaction utilized to transmit the content. Finally, content labels may be stored completely separate from the content in association with an identifier for the content, such as at label bureaus, and retrieved in a separate communications transaction from the content.

With reference now to **Figure 2**, a high level flow chart for a process of setting access control based on content labels in accordance with a preferred embodiment of the present invention is illustrated. The process begins at step **202**, which depicts an access control change being initiated by a privileged user. Verification of the identify of the privileged user (e.g., through a password prompt and check or simply by determining the current user) may optionally be undertaken at this time. The process first passes to step **204**, which illustrates obtaining the content label categories and associated restrictions which define the access control desired for various nonprivileged users. This may be performed using the same user interface dialogs which are currently employed by browsers for setting content label-based restrictions for browsers (e.g., by clicking "Tools", "Internet Options", "Content" for Internet Explorer 5.0).

Once the content label categories and associated user restrictions for the desired access control are obtained, the process then passes to step **206**, which depicts distributing the content label categories and restrictions to all software modules supporting a communications protocols within the system, including FTP, NNTP, instant messaging, SNMP, and other communications protocols. Each communications engine within the system is adapted to receive access control specifications in the form of content label categories and associated user restrictions, and implementing the appropriate access control. By obtaining the content label categories and restrictions once and distributing them among all communications programs within

AUS000072US1

the system, uniform implementation of access controls may be provided with no simple work-arounds such as those which exist in the current systems.

5 Alternatively, content-based restrictions could be implemented through a central source in the operating system, which each communications protocol engine calls with a set of parameters and requests GO/NO GO clearance on access. Thus, an API would be provided to an "access check" which all executable code within the system could employ.

10 Additionally, the content label categories and associated user restrictions are distributed to all communications programs, regardless of the communications protocols employed or when they are installed. Thus, for example, the situation may be avoided in which a parent sets access restrictions for a child for an Internet Explorer Browser installed within the system, but the child subsequently downloads and installs a Netscape Navigator browser on the system to circumvent the restrictions. Communications programs which are installed on the system check for existing access control restrictions set for other communications programs. The process then proceeds to step 208, which illustrates the process becoming idle until another access control change is initiated.

25 With reference now to **Figure 3**, a high level flowchart for a process of performing access control in accordance with a preferred embodiment of the present invention is depicted. The process begins at step 302, which depicts content being requested within a system, utilizing any

AUS000072US1

communications protocol supported by the system, not just a browser employing the HTTP protocol. The process then passes to step 304, which illustrates obtaining content labels for the requested content. As noted above, the content labels may be embedded within the content itself, contained within a communications header for a client-server or similar transaction involved in transmitting the requested content, or looked up in an internal or external database containing content labels for uniquely identified content including the requested content.

The process passes next to step 306, which depicts determining the access restrictions, based on content label categories, which are applicable to a current user. This may optionally involve prompting the user for a password to verify the user's identity or to determine when the user logs onto the system, or may simply entail determining the current user and looking up the access restrictions associated with that user. The process then passes to step 308, which illustrates a determination of whether access to the content label categories including content labels for the requested content is prohibited to the current user. If so, the process proceeds to step 310, which depicts displaying a restricted content message to the user. If not, however, the process proceeds instead to step 312, which illustrates retrieving and displaying the requested content. Display of the requested content may involve playback of audio or video information. From either of steps 310 or 312, the process then passes to step 314, which depicts the process becoming idle until content is again requested via any communications protocol supported within

the system.

5 The present invention allows content-based access control to be readily implemented and uniformly effected across all communications protocols supported by a system. Changes to access restrictions based on content need only be entered by a privileged user once, and are distributed to all communications programs within the system for implementation. Thus, a parent setting access control
10 restrictions for their child in a browser (e.g., Internet Explorer) will have the same access control restrictions automatically set for a newsreader (e.g., Outlook Express) even if the parent is unaware of the existence of the newreader. Communications programs which are later installed check for access restrictions during installation, for example, by checking other communications programs already installed on the system.

20 The present invention allows restriction over access to content, which includes execution of code as well as retrieval and viewing. Control may be provided over all forms of data, whether in files or datastreams or responses to real time requests. Content labeling-based access control may be employed in accordance with the present
25 invention through SmartCards, credit cards, badges, etc. content labeling restrictions for the user of that device.

30 It is important to note that while the present invention has been described in the context of a fully functional data processing system and/or network, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the

AUS000072US1

form of a computer usable medium of instructions in a variety of forms, and that the present invention applies equally regardless of the particular type of signal bearing medium used to actually carry out the distribution.

5 Examples of computer usable mediums include: nonvolatile, hard-coded type mediums such as read only memories (ROMs) or erasable, electrically programmable read only memories (EEPROMs), recordable type mediums such as floppy disks, hard disk drives and CD-ROMs, and transmission type mediums
10 such as digital and analog communication links.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

AUS000072US1

CLAIMS:

What is claimed is:

1 1. A method of access control, comprising:
2 for content accessed by any communications protocol
3 supported within a system, checking for a content label
4 identifying a content category for the content;
5 determining from the content label whether the content
6 is restricted; and
7 responsive to determining from the content label that
8 the content is restricted, prompting a user for a password
9 required to access the content.

1 2. The method of claim 1, wherein the step of checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:
5 checking a content label within the content.

1 3. The method of claim 1, wherein the step of checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:
5 checking a content label within a header for a
6 communications transaction transmitting the content.

1 4. The method of claim 1, wherein the step of checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:
5 checking a label bureau for a content label associated
6 with a uniform resource locator, filename, or datastream

AUS000072US1

1 6. A method of establishing access control, comprising:
2 obtaining content label categories and associated user
3 restrictions for desired access control;
4 distributing the content label categories and
5 associated user restrictions to each of a plurality of
6 communications programs within a system, wherein at least
7 two of the communications programs employ different
8 communications protocols; and
9 setting access controls for each communications program
10 within the system utilizing the content label categories and
11 associated user restrictions.

1 7. The method of claim 6, further comprising:
2 during installation of a communications program
3 subsequent to setting access controls for each
4 communications program within the system utilizing the
5 content label categories and associated user restrictions,
6 checking for existing access control settings for other
7 communications programs and setting access controls for the
8 communications program being installed utilizing the
9 existing access control settings.

AUS000072US1

1 8. A system for access control, comprising:

2 means for checking content accessed by any
3 communications protocol supported within a system for a
4 content label identifying a content category for the
5 content;

6 means for determining from the content label whether
7 the content is restricted; and

8 means, responsive to determining from the content label
9 that the content is restricted, for prompting a user for a
10 password required to access the content.

1 9. The system of claim 8, wherein the means for checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:

5 means for checking a content label within the content.

1 10. The system of claim 8, wherein the means for checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:

5 means for checking a content label within a header for
6 a communications transaction transmitting the content.

1 11. The system of claim 8, wherein the means for checking
2 content accessed by any communications protocol supported
3 within a system for a content label identifying a content
4 category for the content further comprises:

5 means for checking a label bureau for a content label
6 associated with a uniform resource locator or filename for
7 the content.

	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---

AUS000072US1

1 13. A system for establishing access control, comprising:
2 means for obtaining content label categories and
3 associated user restrictions for desired access control;
4 means for distributing the content label categories and
5 associated user restrictions to each of a plurality of
6 communications programs within a system, wherein at least
7 two of the communications programs employ different
8 communications protocols; and
9 means for setting access controls for each
10 communications program within the system utilizing the
11 content label categories and associated user restrictions.

14. The system of claim 13, further comprising:
means operable during installation of a communications
program subsequent to setting access controls for each
communications program within the system utilizing the
content label categories and associated user restrictions
for checking for existing access control settings for other
communications programs and for setting access controls for
the communications program being installed utilizing the
existing access control settings.

AUS000072US1

1 15. A computer program product within a computer usable
2 medium for access control, comprising:

3 instructions for checking content accessed by any
4 communications protocol supported within a system for a
5 content label identifying a content category for the
6 content;

7 instructions for determining from the content label
8 whether the content is restricted; and

9 instructions, responsive to determining from the
10 content label that the content is restricted, for prompting
11 a user for a password required to access the content.

1 16. The computer program product of claim 15, wherein the
2 instructions for checking content accessed by any
3 communications protocol supported within a system for a
4 content label identifying a content category for the content
5 further comprises:

6 instructions for checking a content label within the
7 content.

1 17. The computer program product of claim 15, wherein the
2 instructions for checking content accessed by any
3 communications protocol supported within a system for a
4 content label identifying a content category for the content
5 further comprises:

6 instructions for checking a content label within a
7 header for a communications transaction transmitting the
8 content.

1 18. The computer program product of claim 15, wherein the
2 instructions for checking content accessed by any
3 communications protocol supported within a system for a

AUS000072US1

4 content label identifying a content category for the content
5 further comprises:

6 instructions for checking a label bureau for a content
7 label associated with a uniform resource locator or filename
8 for the content.

1 19. The computer program product of claim 15, wherein the
2 instructions for determining from the content label whether
3 the content is restricted further comprises:

4 instructions for determining one or more content
5 categories from the content label; and

6 instructions for determining whether any content
7 category identified within the content label is restricted
8 for the user.

AUS000072US1

1 20. A computer program product within a computer usable
2 medium for establishing access control, comprising:
3 instructions for obtaining content label categories and
4 associated user restrictions for desired access control;
5 instructions for distributing the content label
6 categories and associated user restrictions to each of a
7 plurality of communications programs within a system,
8 wherein at least two of the communications programs employ
9 different communications protocols; and
10 instructions for setting access controls for each
11 communications program within the system utilizing the
12 content label categories and associated user restrictions.

1 21. The computer program product of claim 20, further
2 comprising:
3 instructions executed during installation of a
4 communications program subsequent to setting access controls
5 for each communications program within the system utilizing
6 the content label categories and associated user
7 restrictions for checking for existing access control
8 settings for other communications programs and for setting
9 access controls for the communications program being
10 installed utilizing the existing access control settings.

EXTENSION OF BROWSER WEB PAGE CONTENT LABELS AND
PASSWORD CHECKING TO COMMUNICATIONS PROTOCOLS

ABSTRACT OF THE DISCLOSURE

Content label categories and associated user
5 restrictions for desired access control may be entered by a
privileged user in any communications programs (such as a
browser) within a system, and are automatically distributed
to all other communications programs (such as a different
browser or a newsreader) within the system regardless of
whether the same communications protocol is utilized.
10 Communications programs being installed check for access
control settings within other communications programs or via
a common API in a centrally located operating system access
control support function, and employ such settings in
15 configuring internal access controls. Content-based access
control is thus implemented uniformly across the system
without work arounds being available to the nonprivileged
users. Content labels for requested content, which may be
embedded within the requested content, contained within a
20 communications header for transactions bearing the requested
content, or looked up in internal or external databases
utilizing an identifier for the requested content, are
checked against content label categories restricted for a
current user. If restricted content is detected, the user
25 is prompted for a password before the requested content is
displayed.

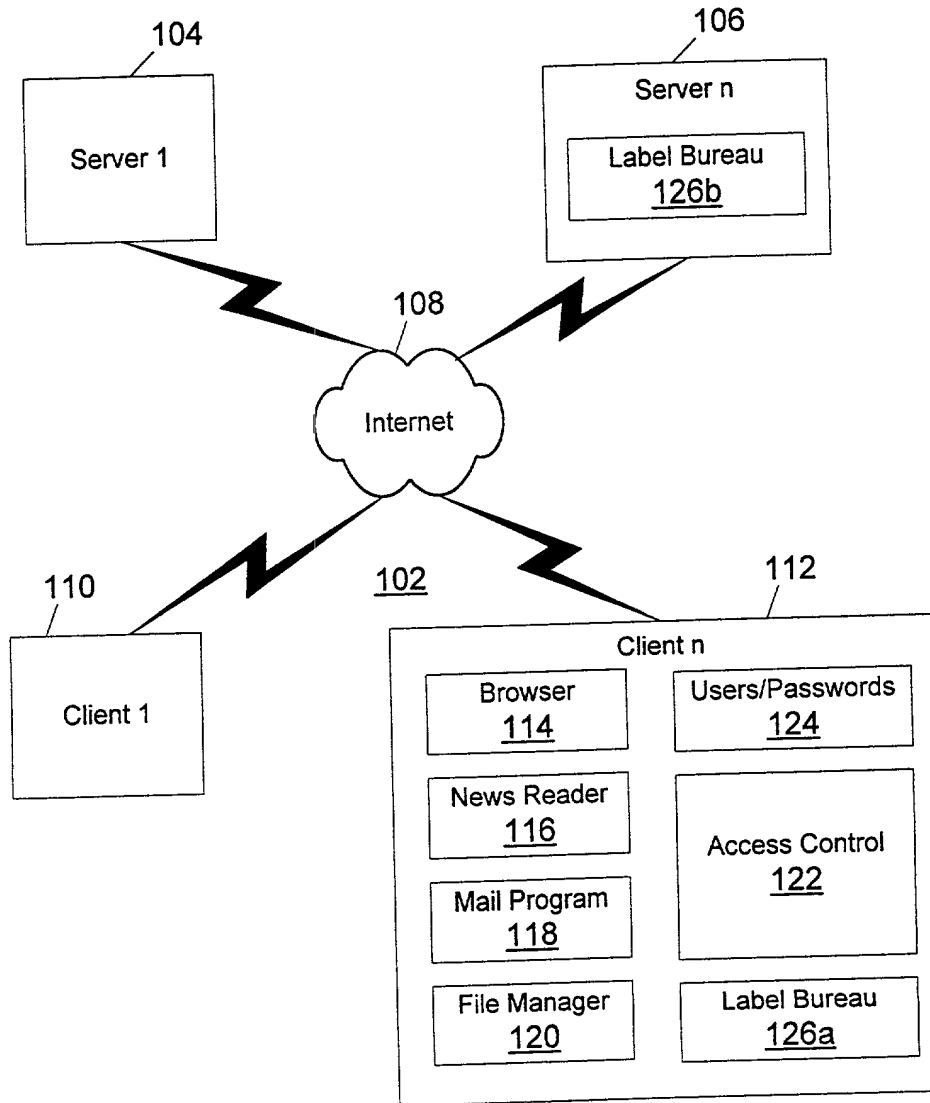


Figure 1

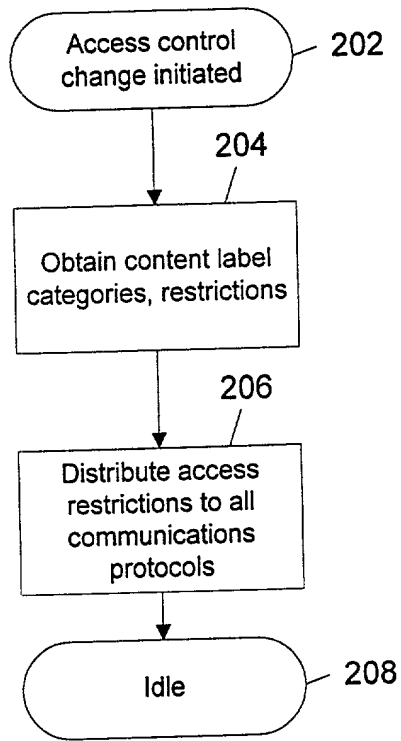


Figure 2

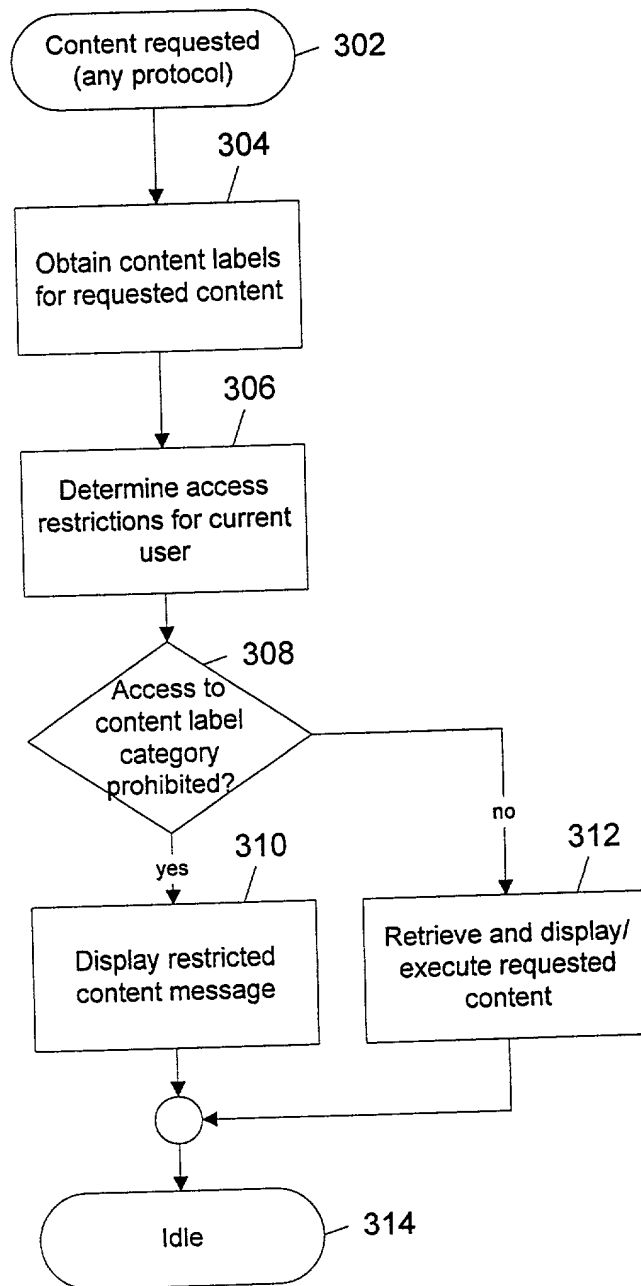


Figure 3

DECLARATION AND POWER OF ATTORNEY FOR

PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

EXTENSION OF BROWSER WEB PAGE CONTENT LABELS AND
PASSWORD CHECKING TO COMMUNICATIONS PROTOCOLS

the specification of which (check one)

X is attached hereto.

_____ was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s): _____ Priority Claimed

_____ Yes _____ No
(Number) (Country) (Day/Month/Year)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Serial #) _____ (Filing Date) _____ (Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John W. Henderson, Jr., Reg. No. 26,907; Thomas E. Tyson, Reg. No. 28,543; Robert M. Carwell, Reg. No. 28,499; Jeffrey S. LaBaw, Reg. No. 31,633; Douglas H. Lefevre, Reg. No. 26,193; Casimer K. Salys, Reg. No. 28,900; David A. Mims, Jr., Reg. No. 32,708; Mark E. McBurney, Reg. No. 33,114; Volel Emile, Reg. No. 39,969; James H. Barksdale, Jr. Reg. No. 24,091; Anthony V. England, Reg. No. 35,129; Leslie A. Van Leeuwen, Reg. No. 42,196; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; and Joseph C. Redmond, Jr., Reg. No. 18,753; Marilyn S. Dawkins, Reg. 31,140; Andrew Mitchell Harris, Reg. No. 42,638; Richard N. McCain, Reg. No. 43,785; Andrew J. Dillon, Reg. No. 29,634; Max Cicccarelli, Reg. No. 39,454; Jack V. Musgrove, Reg. No. 31,986; Daniel E. Venglarik, Reg. No. 39,409; Brian F. Russell, Reg. No. 40,796; John G. Graham, Reg. No. 19,563; Matthew W. Baca, Reg. No. 42,277; Justin M. Dillon, Reg. No. 42,486; Antony P. Ng, Reg. No. 43,427; Steven Lin, Reg. No. 35,250; Matthew S. Anderson, Reg. No. 39,093; Sidney L. Weatherford, Reg. No. P45,602; and Mike Noe, Reg. No. 44,975.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Lakewood on the Park, Suite 350, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, 512/343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: Randolph Michael Forlenza

INVENTORS SIGNATURE: Randolph M. Forlenza DATE: 4/7/00

RESIDENCE: 5807 Standing Rock Drive
Austin, Texas 78730

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 5807 Standing Rock Drive
Austin, Texas 78730

FULL NAME OF SOLE OR SECOND INVENTOR: Miguel Sang

INVENTORS SIGNATURE: Miguel Seng DATE: 4/7/2010

RESIDENCE: 3401 Parmer Lane, Apt. 628 5817 MIRAMONTE DR
Austin, Texas 78727 AUSTIN, TX 78759

CITIZENSHIP: ~~U.S.A.~~ DOMINICAN REPUBLIC

POST OFFICE ADDRESS: 3401 Parmer Lane, Apt. 628 MIGUEL SA 5817 MIRAMONTE DR
Austin, Texas 78727 AUSTIN, TX 78759

Fort Worth/0116AD-37561/79123.1